Creating Self-signed Certificate for Trusted HTTPS Connection

For **NPort 6150-G2-T** with **Mozilla Firefox** and **OpenSSL** on **Ubuntu 24.04 LTS Server**

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Jun 23, 2026

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 35 years of industry experience, Moxa has connected more than 111 million devices worldwide and has a distribution and service network that reaches customers in more than 91 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

1 Purpose and Scope

This guide describes how to create a self-signed certificate for a trusted and encrypted HTTPS connection to the embedded web server of an **NPort 6150-G2-T**. The certificate is generated with **OpenSSL** on **Ubuntu 24.04 LTS Server**, imported into the NPort-G2 device, and the CA certificate is imported into **Mozilla Firefox** so that the browser trusts the device HTTPS connection.

The procedure includes:

- Preparing the Ubuntu server's time zone.
- Creating OpenSSL configuration files.
- Creating a CA certificate and private key.
- Creating the NPort-G2 HTTPS server certificate.
- Importing the certificate into the NPort-G2 device.
- Importing the CA certificate into Mozilla Firefox.
- Verifying that the browser trusts the NPort-G2 web server.

2 Test Bench Environment

The following environment was used to validate the configuration.

Table 1: Validated test bench

Component	Version/Details
Ubuntu Server	Ubuntu 24.04.4 LTS; Linux kernel 6.8.0-107-generic
OpenSSL on Linux	OpenSSL 3.0.13, 30 Jan 2024
NPort Device	NPort 6150-G2-T; firmware 1.2.0 Build 26042302
Mozilla Firefox	150.0.3 (64-bit)
NPort 6150-G2-T IP-Address	192.168.127.254/24

3 Prerequisites

Before starting, make sure that:

- You have shell access to the Ubuntu server.
- OpenSSL is available on the Ubuntu server.
- You have administrative access to the NPort-G2 web interface.
- The NPort-G2 device's IP address is known.
- The system time on the Ubuntu server and on the NPort-G2 device is correct.

IMPORTANT

Certificate validation is time-sensitive. Incorrect date, time, or time zone settings can cause the browser or device to reject the certificate.

4 Set the Time Zone on Ubuntu 24.04 LTS Server

4.1 Set the Time Zone

Set the Ubuntu server's time zone. This example uses Europe/Berlin.

```
$ sudo timedatectl set-timezone Europe/Berlin
```

4.2 Verify the Time Zone

Verify the configured time zone and current time.

```
$ timedatectl
```

Expected output:

```
Local time: Thu 2026-05-21 16:23:57 CEST
Universal time: Thu 2026-05-21 14:23:57 UTC
RTC time: Thu 2026-05-21 14:23:57
Time zone: Europe/Berlin (CEST, +0200)
System clock synchronized: no
NTP service: active
RTC in local TZ: no
```

5 Create the Self-signed Certificate for NPort-G2 HTTPS

5.1 Create the OpenSSL Working Directory

Create a directory in the home directory for the certificates and change into it.

```
$ mkdir CA_NPort_SSL-HTTPS
$ cd CA_NPort_SSL-HTTPS
```

Copy the default OpenSSL configuration file to the working directory.

```
$ cp /etc/ssl/openssl.cnf .
```

5.2 Edit openssl.cnf

Open the copied OpenSSL configuration file.

```
$ nano openssl.cnf
```

In the **[v3_ca]** section, verify or set the following values.

```
authorityKeyIdentifier=keyid:always,issuer

# Key usage: this is typical for a CA certificate. However since it will
# prevent it being used as an test self-signed certificate it is best
# left out by default.
keyUsage = critical, cRLSign, keyCertSign
```

In the **[CA_default]** section, set the working directory.

```
dir = .     # Where everything is kept
```

5.3 Create cert.conf

Create the **cert.conf** file.

```
$ nano cert.conf
```

Add the following certificate extension configuration.

```
authorityKeyIdentifier = keyid, issuer
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName = @alt_names

[alt_names]
IP.1  =  192.168.127.254              # IP-Address of the NPort -G2
DNS.1 = NPort-6150-G2.meuts.lan       # Hostname of the NPort -G2
```

Note In a production environment, the Subject Alternative Name should contain the IP address if no DNS server is available. If a DNS server is available, the Subject Alternative Name should contain the hostname of the Moxa device. This example includes both values.

5.4 Create csr.conf

Create the **csr.conf** file.

```
$ nano csr.conf
```

Add the following CSR configuration.

```
[  req  ]
default_bits = 2048
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C = DE
ST = Bayern
L  =  Eching
O = MEU
OU = MEU-TS
CN = Server-SSL-HTTPS-Certificate
emailAddress = info@moxa.com
```

5.5 Create the CA Certificate and Key

Create the CA private key and CA certificate.

```
$ openssl req -x509 -sha256 -nodes -newkey rsa:2048 -keyout CA.key \
-out CA.crt -days 365 -config openssl.cnf
```

Example input values:

```
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Bayern
Locality Name (eg, city) []:Munich
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MEU
Organizational Unit Name (eg, section) []:MEU-TS
Common Name (e.g. server FQDN or YOUR name) []:CA-Cert-SSL-HTTPS
Email Address []:
```

5.6 Create the HTTPS Server Certificate for NPort-G2

The NPort-G2 device acts as the HTTPS server. Generate the server private key.

```
$ openssl genrsa -out Server.key 2048
```

Generate the Certificate Signing Request (CSR) by using the server private key.

```
$ openssl req -new -key Server.key -out Server.csr -config csr.conf
```

Generate the server HTTPS certificate.

```
$ openssl x509 -req -in Server.csr -CA CA.crt -CAkey CA.key \
-CAcreateserial -out Server.pem -days 360 -sha256 -extfile cert.conf
```

Expected output:

```
Certificate request self-signature ok
subject=C = DE, ST = Bayern, L = Eching, O = MEU, OU = MEU-TS, CN =
Server-SSL-HTTPS-Certificate, emailAddress = info@moxa.com
```

Merge the server private key and server certificate into a single PEM file for the NPort-G2 device.

```
$ cat Server.key Server.pem > NPort-G2_SSL-HTTPS_Key_Pem.pem
```

6 Useful OpenSSL Commands

The following OpenSSL commands can help verify certificate files during troubleshooting.

```
# Check a Certificate Signing Request (CSR)
openssl req -text -noout -verify -in CSR.csr

# Check a private key
openssl rsa -in privateKey.key -check

# Check a certificate
openssl x509 -in certificate.crt -text -noout

# Export PEM and key into a PFX file
openssl pkcs12 -export -out Server.pfx -inkey Server.key -in Server.pem

# Display the contents of a PFX/P12 file
openssl pkcs12 -in example.pfx -info
```

Note **Common Name vs. Subject Alternative Name**

The common name can only contain one entry. The Subject Alternative Name (SAN) extension allows multiple names or IP addresses and is the modern reference used by browsers for HTTPS certificate validation. For HTTPS certificates, SAN should be used for the server identity.

7 Configure the NPort-G2 Device and Mozilla Firefox

7.1 Set the Time, Date, and Time Zone on the NPort-G2

Set the time zone and daylight saving time on the NPort-G2 device by navigating to **System Settings > General > Date & Time**.

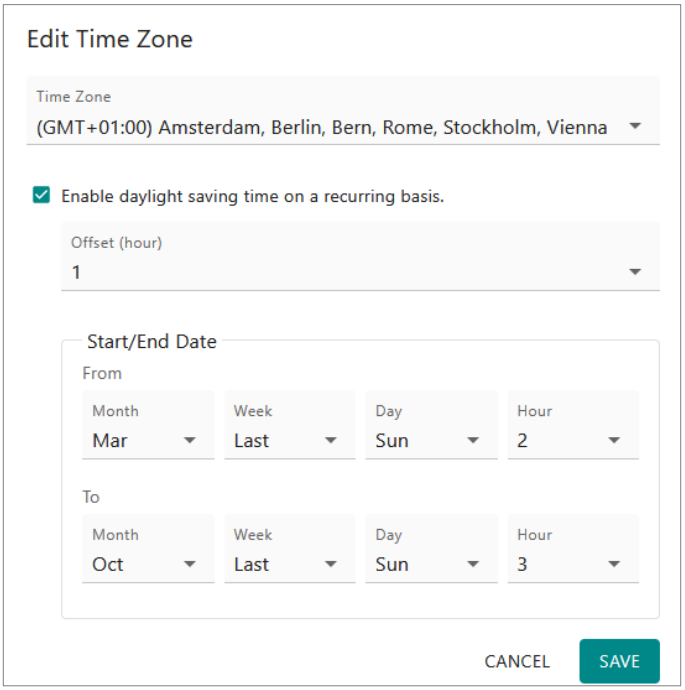

Figure 1: Configure the *NPort-G2 time zone and daylight saving settings*

Set the current date and time to local time in **System Settings > General > Date & Time**.

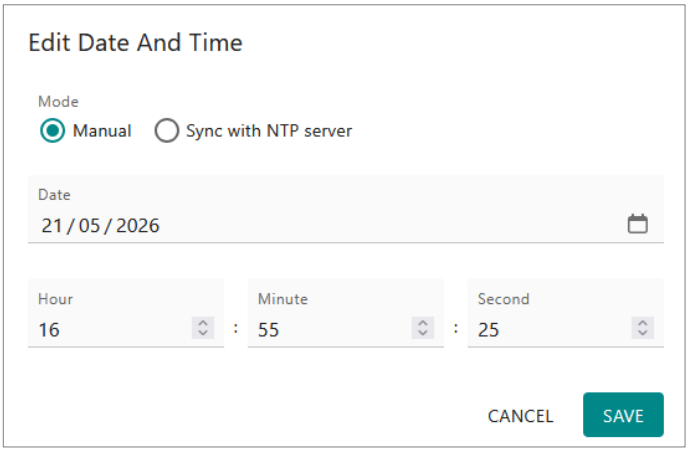

Figure 2: Configure the *NPort-G2 date and time*

7.2 Import the Self-signed Certificate Into the NPort-G2

Import the created certificate file NPort-G2_SSL-HTTPS_Key_Pem.pem into the NPort-G2 device by navigating to **Security > Certificate > MANAGE > Import user certificate**.

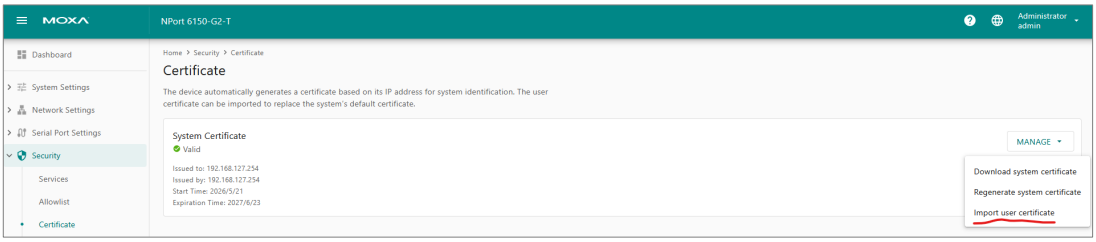

Figure 3: Open the NPort-G2 user certificate import function

After the NPort-G2 device reboots, verify the status of the imported certificate.

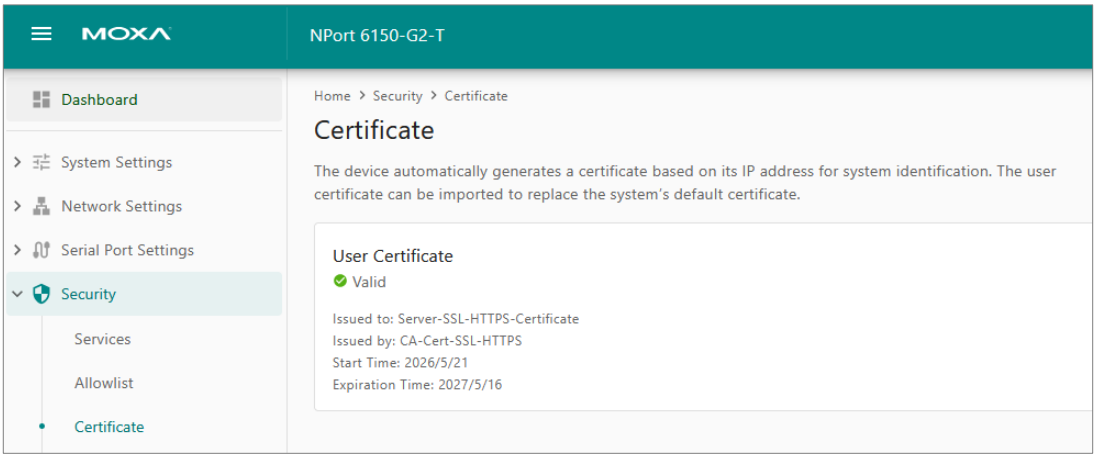

Figure 4: Verify the imported NPort-G2 user certificate status

7.3 Import the CA Certificate Into Mozilla Firefox

Open Mozilla Firefox, select the hamburger menu in the upper-right corner, and then **Settings**.

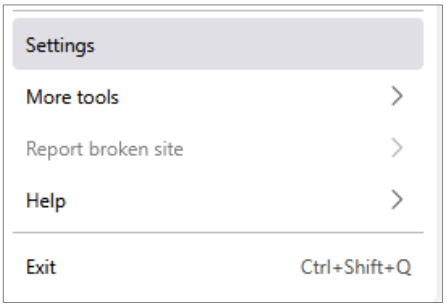

Figure 5: Open Firefox settings

Select **Privacy & Security** in the left-hand menu.

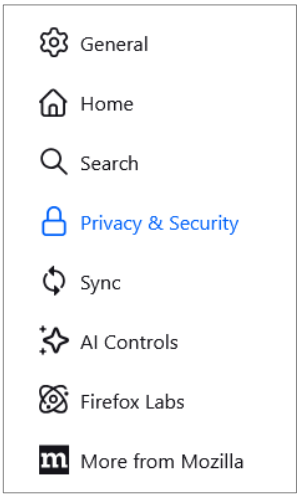

Figure 6: Open the Firefox Privacy and Security menu

Scroll down to **Certificates** and select **Manage certificates**.

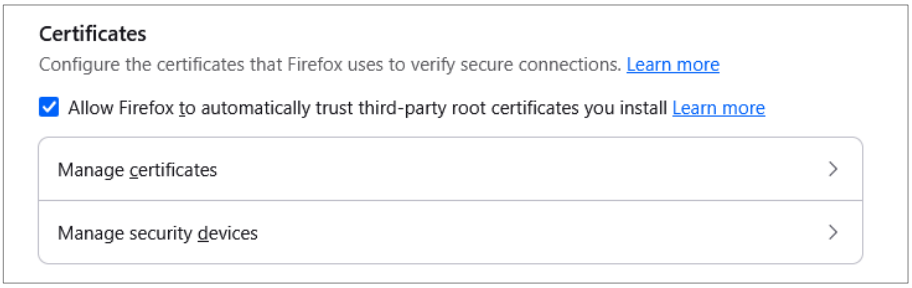

Figure 7: Open Firefox certificate management

Select **Import...** and import the recently created `CA.crt` file.

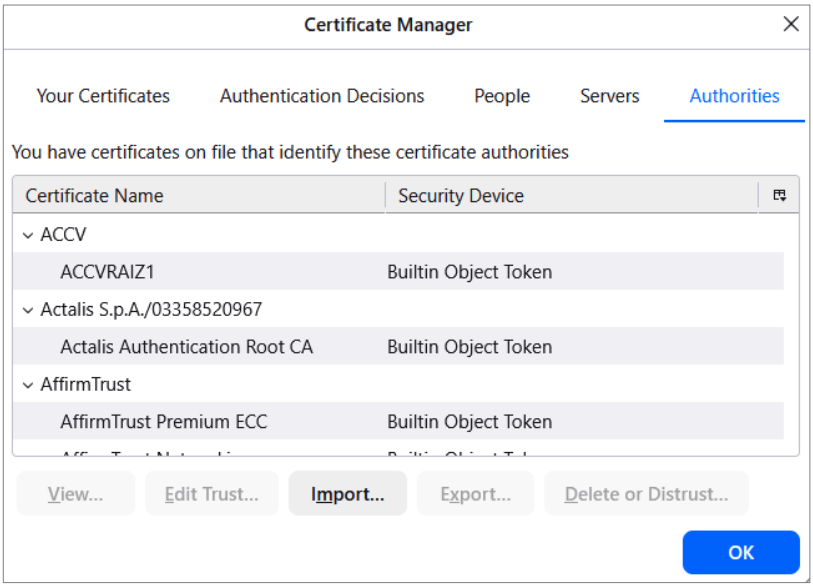

Figure 8: Import the CA certificate into Firefox

Select **Trust this CA to identify websites,** and then **OK**.

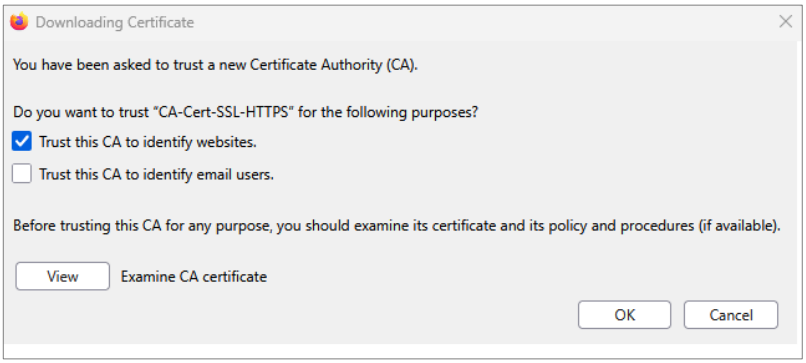

Figure 9: Trust the imported CA for website identification

Scroll down to the **MEU** certificate name and verify that the imported **CA-Cert-SSL-HTTPS** certificate is listed.

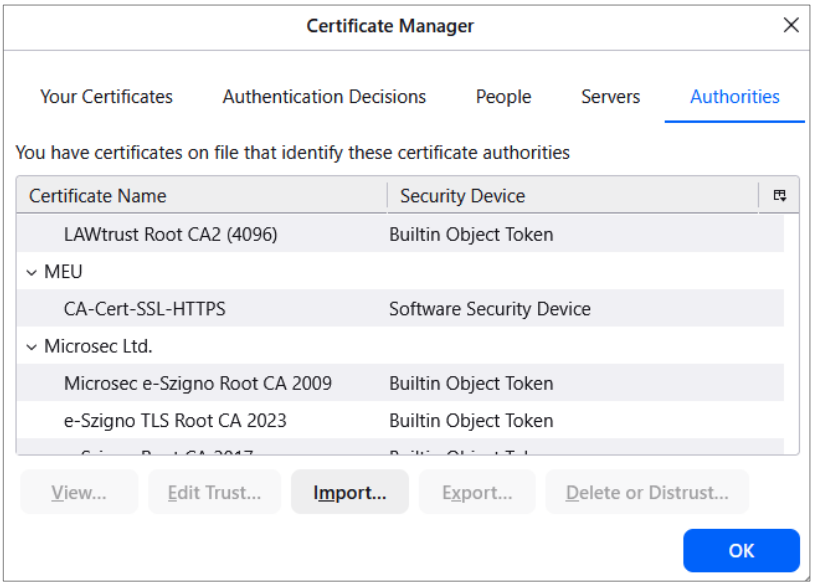

Figure 10: Verify the imported CA certificate in Firefox

Refresh the NPort-G2 web page in Mozilla Firefox. The shield icon in front of the address bar shows that the NPort-G2 embedded web server is trusted.

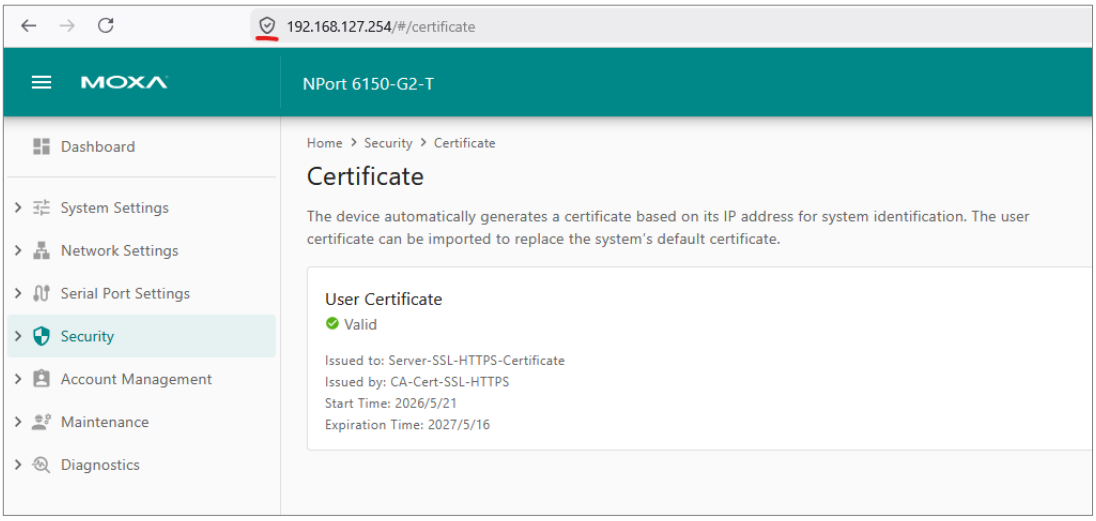

Figure 11: Verify the trusted HTTPS connection to the NPort-G2 web server

8 Verification Checklist

Use the following checklist to validate the deployment.

- The Ubuntu server's time and time zone are correct.
- The CA certificate **CA.crt** was created successfully.
- The server certificate **Server.pem** was created successfully.
- The combined file **NPort-G2_SSL-HTTPS_Key_Pem.pem** was imported into the NPort-G2 device.
- The NPort-G2 device shows the imported user certificate as valid.
- The CA certificate **CA.crt** was imported into Firefox Authorities.
- Firefox is configured to trust the CA for website identification.
- The NPort-G2 HTTPS page opens as trusted in Firefox.